Specifiche tecniche previste dall'articolo 34, comma 1 del decreto del Ministro della giustizia in data 21 febbraio 2011 n. 44, recante regolamento concernente le regole tecniche per l'adozione, nel processo civile e nel processo penale, delle tecnologie dell'informazione e della comunicazione, in attuazione dei principi previsti dal decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni, ai sensi dell'articolo 4, commi 1 e 2 del decreto-legge 29 dicembre 2009, n. 193, convertito nella legge 22 febbraio 2010, n. 24

MINISTERO DELLA GIUSTIZIA

Dipartimento per la transizione digitale della giustizia, l'analisi statistica e le politiche di coesione

Direzione generale per i sistemi informativi automatizzati

IL DIRETTORE GENERALE

Visto il decreto del Ministro della giustizia in data 21 febbraio 2011, n. 44, recante "Regolamento concernente le regole tecniche per l'adozione nel processo civile e nel processo penale delle tecnologie dell'informazione e della comunicazione, in attuazione dei principi previsti dal decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni, ai sensi dell'articolo 4, commi 1 e 2, del decreto-legge 29 dicembre 2009, n. 193, convertito nella legge 22 febbraio 2010 n.24", come modificato dal decreto del Ministro della giustizia 15 ottobre 2012, n. 209, dal decreto del Ministro della giustizia 3 aprile 2013, n. 48 e dal decreto del Ministro della giustizia 29 dicembre 2023, n. 217;

Visto il decreto legislativo 30 giugno 2003, n. 196, recante "Codice in materia di protezione dei dati personali" e successive modificazioni;

Visto il decreto legislativo 7 marzo 2005, n. 82, recante "Codice dell'amministrazione digitale" e successive modificazioni;

Visto il decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, recante "Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge n. 16 gennaio 2003, n. 3";

Visto il decreto del Ministro della giustizia 27 aprile 2009 recante "Nuove regole procedurali relative alla tenuta dei registri informatizzati dell'amministrazione della giustizia";

Visto il decreto-legge 18 ottobre 2012, n. 179, recante "Ulteriori misure urgenti per la crescita del Paese", convertito con modificazioni dalla legge 17 dicembre 2012, n. 22;

Visto il decreto legislativo 10 ottobre 2022, n. 149, recante "Attuazione della legge 26 novembre 2021, n. 206, recante delega al Governo per l'efficienza del processo civile e per la revisione della disciplina degli strumenti di risoluzione alternativa delle controversie e misure urgenti di razionalizzazione dei procedimenti in materia di diritti delle persone e delle famiglie nonché in materia di esecuzione forzata";

Visto il decreto legislativo 10 ottobre 2022, n. 150, recante "Attuazione della legge 27 settembre 2021, n. 134, recante delega al Governo per l'efficienza del processo penale, nonché in materia di giustizia riparativa e disposizioni per la celere definizione dei procedimenti giudiziari";

Visto l'articolo 36 del decreto-legge 24 febbraio 2023, n. 13, recante "Disposizioni urgenti per l'attuazione del Piano nazionale di ripresa e resilienza (PNRR) e del Piano nazionale degli investimenti complementari al PNRR (PNC), nonché per l'attuazione delle politiche di coesione e della politica agricola comune", convertito con modificazioni dalla legge 21 aprile 2023, n. 41;

Rilevata la necessità di adottare nuove specifiche tecniche previste dall'articolo 34, comma 1, del decreto del Ministro della giustizia 21 febbraio 2011, n. 44, come da ultimo novellato dal decreto del Ministro della giustizia 29 dicembre 2023, n. 217;

Acquisito il parere espresso in data XXX dal Garante per la protezione dei dati personali;

Acquisito il parere espresso in data XXX dall'Agenzia per l'Italia Digitale;

EMANA

IL SEGUENTE PROVVEDIMENTO

CAPO I

PRINCIPI GENERALI

Articolo 1

(Ambito di applicazione)

1. Il presente provvedimento stabilisce le specifiche tecniche previste dall'articolo 34, comma 1, del regolamento concernente le regole tecniche per l'adozione nel processo civile e nel processo penale delle tecnologie dell'informazione e della comunicazione, in attuazione dei principi previsti dal decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni, ai sensi dell'articolo 4, commi 1 e 2, del decreto-legge 29 dicembre 2009, n. 193, convertito nella legge 22 febbraio 2010 n.24.

Articolo 2

(Definizioni)

1. Ai fini del presente provvedimento, oltre alle definizioni contenute nell'articolo 2 del Regolamento, si intende:

a) Annotazioni Preliminari dal Portale: area di transito del Re.Ge.WEB nella quale sono effettuati i controlli preliminari sulle comunicazioni di cui all'articolo 17 dal personale di segreteria degli uffici del pubblico ministero;
   Area Riservata: contenitore di tutte le pagine e i servizi del Portale dei Servizi telematici disponibili previa identificazione informatica come disciplinata dall'articolo 5 delle specifiche tecniche;
b) Atto Abilitante: atto da cui risulti la conoscenza dell'esistenza in una procura della Repubblica di un procedimento relativo al proprio assistito e il relativo numero di registro;

c) Autenticazione a due fattori: metodo di autenticazione che si basa sull'utilizzo congiunto di due metodi di autenticazione individuale, ossia che combina un'informazione nota (ad esempio un nome utente e una password) con un oggetto a disposizione (ad esempio, una carta di credito, token o telefono cellulare).

d) PDF: Portable Document Format;

e) PDP: Portale Deposito atti Penali di cui all'articolo 7-*bis*, comma 1, del Regolamento;

f) PNR: Portale delle notizie di reato di cui all'articolo 7-*bis*, comma 2, del Regolamento;

g) PST: Portale Servizi Telematici di cui all'articolo 6 del Regolamento;

h) CAD: decreto legislativo 7 marzo 2005, n. 82, recante "Codice dell'amministrazione digitale" e successive modificazioni;

i) CAdES (CMS Advanced Electronic Signature): formato di busta crittografica definito nella norma ETSI TS 101 733 V1.7.4 e basata a sua volta sulle specifiche RFC 3852 e RFC 2634 e successive modificazioni;

j) Certificato: documento digitale generato da EJBCA, dietro specifica approvazione da parte di personale autorizzato;

k) CNS: Carta Nazionale dei Servizi;

l) CSV: Comma-separated values;

m) DTD: Document Type Definition;

n) DGSIA: Direzione generale per i sistemi informativi automatizzati del Dipartimento per la transizione digitale l'analisi statistica e le politiche di coesione del Ministero della giustizia;

o) EJBCA: software di Certification Authority;

p) Funzione di hash: una funzione matematica che genera, a partire da un documento informatico, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire il documento informatico originario e generare impronte uguali a partire da documenti informatici differenti;

q) GSU: Sistema di gestione informatizzata dei registri per gli uffici notifiche e protesti;

r) HSM: Hardware Security Module;

s) HTTPS: HyperText Transfer Protocol over Secure Socket Layer;

t) IMAP: Internet Message Access Protocol;

u) Impronta: la sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione di una opportuna funzione di hash.

v) OID (Object IDentifier): codice univoco basato su una sequenza ordinata di numeri per l'identificazione di evidenze informatiche utilizzate per la rappresentazione di oggetti come estensioni, attributi, documenti e strutture di dati in genere nell'ambito degli standard internazionali relativi alla interconnessione dei sistemi aperti che richiedono un'identificazione univoca in ambito mondiale;

w) PAdES (PDF Advanced Electronic Signature): formato di busta crittografica definito nella norma ETSI TS 102 778 basata a sua volta sullo standard ISO/IEC 32000 e successive modificazioni;

x) PdA: Punto di accesso, come definito all'articolo 23 del regolamento;

y) PEC: Posta Elettronica Certificata;

z) PKCS#11: interfaccia di programmazione che consente di accedere alle funzionalità crittografiche del token; tramite apposita sequenza di chiamate al token per mezzo dell'interfaccia PKCS#11 è possibile implementare la procedura di identificazione;

aa) POP: Post Office Protocol;

bb) RAFE (Registration Authority Front End): software in uso al personale autorizzato per la gestione dei certificati. Si connette a EJBCA per la generazione e la revoca dei certificati;

cc) Regolamento: il decreto del Ministro della giustizia in data 21 febbraio 2011, n. 44, recante "Regolamento concernente le regole tecniche per l'adozione nel processo civile e nel processo penale delle tecnologie dell'informazione e della comunicazione, in attuazione dei principi previsti dal decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni, ai sensi dell'articolo 4, commi 1 e 2, del decreto-legge 29 dicembre 2009, n. 193, convertito nella legge 22 febbraio 2010 n. 24" e successive modificazioni;

dd) RdA: Ricevuta di accettazione della posta elettronica certificata;

ee) RdAC: Ricevuta di avvenuta consegna della posta elettronica certificata;

ff) Re.Ge.WEB: modulo del sistema SICP per la gestione dei registri di cancelleria;

gg) ReGIndE: Registro Generale degli Indirizzi Elettronici, come definito all'articolo 7 del regolamento;

hh) SICP: Sistema Informativo della Cognizione Penale;

ii) SMTP: Simple Mail Transfer Protocol;

jj) SPC: Sistema Pubblico di Connettività;

kk) SPID: sistema pubblico di identità digitale;

ll) Ufficio Fonte: struttura organizzativa nella quale sono inseriti dipendenti con le qualifiche di Ufficiali o Agenti di Polizia Giudiziaria.

mm) UNEP: Ufficio Notificazioni, Esecuzioni e Protesti;

nn) WSDL: Web Services Definition Language;

oo) XML; eXtensible Markup Language;

pp) XSD: XML Schema Definition.

CAPO II

SISTEMI INFORMATICI DEL DOMINIO GIUSTIZIA

Articolo 3

(Infrastrutture informatiche)

1. Il sistema informatico del Ministero della giustizia è articolato, salvo le infrastrutture unitarie e comuni, a livello nazionale, interdistrettuale e distrettuale. In fase transitoria e quando ragioni tecniche lo rendono assolutamente necessario, possono essere mantenute strutture a livello locale (di circondario).

2. Fermo quanto previsto da altre disposizioni, costituiscono infrastrutture unitarie e comuni le banche dati e i sistemi informatici indicati nell'allegato 1.

3. Il sistema di posta elettronica certificata è gestito dal fornitore presso la propria sala server, collegata a SPC secondo le relative regole di interoperabilità e sicurezza, oppure presso una sala server del Ministero della giustizia.

4. Il dispiegamento di detti sistemi rispetta le disposizioni di cui al decreto del Ministro della giustizia in data 27 aprile 2009, recante "Nuove regole procedurali relative alla tenuta dei registri informatizzati dell'amministrazione della giustizia".

5. Il Direttore generale DGSIA emana ed aggiorna periodicamente, con proprio decreto, le linee guida per la organizzazione e gestione del sistema informatico, sentito il Garante per la protezione dei dati personali. Le linee guida sono rese note con gli opportuni strumenti di comunicazione ed in ogni caso sul sito internet dell'Amministrazione.

6. Le strutture elaborative serventi ed i dati sono allocati in corrispondenza delle componenti di cui ai commi precedenti.

Articolo 4

(Gestore della posta elettronica certificata del Ministero della giustizia)

1. Il Ministero della giustizia si avvale del proprio gestore di posta elettronica certificata, che rilascia e gestisce apposite caselle di PEC degli uffici giudiziari e degli UNEP da utilizzare esclusivamente per i servizi previsti dal regolamento, nel rispetto delle specifiche tecniche riportate nel presente provvedimento.

2. Le caselle appartengono ad apposito sotto-dominio (civile.ptel.giustiziacert.it e penale.ptel.giustiziacert.it) e possono ricevere unicamente messaggi di posta elettronica certificata. I messaggi di posta elettronica ordinaria vengono automaticamente scartati.

3. Il gestore dei servizi telematici utilizza i protocolli POP3, POP3S, IMAP, IMAPS e SMTP per collegarsi al gestore di posta elettronica certificata del Ministero.

4. La codifica dei singoli uffici, comprensiva del relativo indirizzo di PEC, è contenuta nel catalogo dei servizi telematici di cui all'articolo 5, comma 3.

5. Non possono essere utilizzate caselle di PEC diverse da quelle di cui ai commi precedenti per la trasmissione e il deposito di atti processuali.

6. Il Ministero della giustizia conserva il log dei messaggi, transitati attraverso il proprio gestore di posta elettronica certificata, per cinque anni. A tal fine, il gestore di PEC del Ministero invia giornalmente, a una casella di posta di sistema, il log in formato CSV. Il log, sottoscritto con firma digitale o firma elettronica qualificata, è relativo a tutti gli indirizzi del sotto-dominio delle caselle del processo telematico e contiene tutti gli eventi relativi ai messaggi pervenuti, conservando le seguenti informazioni:

a) il codice identificativo univoco assegnato al messaggio originale;

b) la data e l'ora dell'evento;

c) il mittente del messaggio originale;

d) i destinatari del messaggio originale;

e) l'oggetto del messaggio originale;

f) il tipo di evento (accettazione, ricezione, consegna, emissione ricevute, errore, ecc.);

g) il codice identificativo dei messaggi correlati generati (ricevute, errori, ecc.);

h) il gestore mittente.

7. Un apposito modulo nell'ambito del PST comprende i componenti funzionali necessari per l'acquisizione, il salvataggio e l'interrogazione dei log prodotti dal servizio di PEC.

8. I web service d'interrogazione dei log PEC sono disponibili ai sistemi interni al dominio Giustizia.

9. Le comunicazioni di atti e documenti tra l'ufficio del pubblico ministero e gli ufficiali ed agenti di polizia giudiziaria nella fase delle indagini preliminari, avvengono anche mediante i gestori di posta elettronica certificata delle forze di polizia; in questo caso il gestore dei servizi telematici utilizza un canale sicuro protetto da un meccanismo di crittografia mediante i protocolli POP3Ss o HTTPS, al fine di evitare la trasmissione in chiaro delle credenziali di accesso e dei messaggi.

Articolo 5

(Portale dei servizi telematici)

1. Il PST è accessibile all'indirizzo https://pst.giustizia.it ed è composto di una "area pubblica" e di una "area riservata".

2. L'area pubblica, denominata "Servizi online Uffici Giudiziari", è composta da tutte le pagine web e i servizi del portale disponibili ad accesso senza l'impiego di apposite credenziali, sistemi di identificazione e requisiti di legittimazione; in essa sono disponibili le seguenti tipologie d'informazione:

a) Informazioni e documentazione sui servizi telematici del dominio giustizia;

b) Raccolte giurisprudenziali;

c) Informazioni essenziali sullo stato dei procedimenti pendenti, rese disponibili in forma anonima; in questo caso, i parametri e i risultati di ricerca riportano unicamente i dati identificativi dei procedimenti (numero di ruolo, numero di sentenza, ecc.), senza riferimenti in chiaro ai nomi o ai dati personali delle parti e tali per cui non sia possibile risalire all'identità dell'interessato. Il canale di comunicazione per l'accesso a tali informazioni è cifrato (HTTPS).

3. Nell'area pubblica è consultabile il catalogo dei servizi telematici, che si compone di una serie di file aventi lo scopo di censire, in forma strutturata, tutte le informazioni relative ai servizi telematici, secondo gli XSD di cui all'Allegato 10.

4. Per area riservata s'intende il contenitore di tutte le pagine e i servizi del portale disponibili previa identificazione informatica, come disciplinata dall'articolo 6.

5. Nell'area riservata sono disponibili informazioni, dati e provvedimenti giudiziari in formato elettronico, secondo quanto previsto all'art. 27 del regolamento, nonché i servizi di pagamento telematico e di richiesta copie.

Articolo 6

(Identificazione informatica)

1. L'identificazione informatica per i soggetti abilitati esterni e gli utenti privati avviene sul PST mediante carta nazionale dei servizi e sul punto di accesso mediante autenticazione a due fattori oppure tramite token crittografico (smart card, chiavetta USB o altro dispositivo sicuro) o SPID, in conformità all'articolo 64 del decreto legislativo 7 marzo 2005, n. 82; in caso si utilizzi il token crittografico, l'identificazione avviene nel rispetto dei seguenti requisiti:

a) Il certificato deve essere rilasciato da un certificatore accreditato dall'Agenzia per l'Italia Digitale ai sensi dell'art 29 del CAD, che si fa garante dell'identità del soggetto;

b) Il certificato deve rispettare il profilo del certificato previsto dalla Carta Nazionale dei Servizi (CNS), facendo riferimento all'Appendice 1 del documento rilasciato dal CNIPA: "Linee guida per

l'emissione e l'utilizzo della Carta Nazionale dei Servizi". L'estensione Certificate Policy (2.5.29.32) può essere valorizzata con un Object Identifier (OID) definito dalla CA;

c) In termini di sicurezza, i dispositivi ammessi sono i dispositivi personali consentiti per la firma elettronica qualificata e quindi smart card e token USB, secondo quanto previsto dalla normativa vigente. I dispositivi sicuri devono essere certificati Common Criteria EAL4+ con traguardo di sicurezza o profilo di protezione conforme alle disposizioni comunitarie;

d) In termini d'interoperabilità, sono ammissibili dispositivi che consentano la disponibilità di entrambe le interfacce PKCS#11 e CSP; in particolare, entrambe le interfacce devono consentire l'accesso alla procedura d'identificazione forte mediante digitazione del PIN da parte dell'utente; il dispositivo deve inoltre rispettare la strutturazione del file system come da specifiche CNS.

2. In fase di identificazione tramite token crittografico, il punto di accesso o il PST verifica la validità del certificato presente nel token crittografico utilizzato dall'utente che accede; prima di consentire qualunque operazione, inoltre, il punto di accesso verifica che il token crittografico sia collegato alla postazione; in caso contrario, invalida e termina la sessione.

3. Il Ministero della giustizia verifica, anche attraverso opportune visite ispettive, che i punti di accesso rispettino i predetti requisiti.

4. La violazione di queste regole di sicurezza comporta per il punto di accesso la sospensione dell'autorizzazione a erogare i servizi, fino al definitivo rispetto dei requisiti.

5. L'identificazione informatica per i soggetti abilitati interni avviene ai sensi dell'articolo 12.

Articolo 7

(Registro generale degli indirizzi elettronici)

1. Il ReGIndE è gestito dal Ministero della giustizia e contiene i dati identificativi nonché l'indirizzo di PEC dei soggetti abilitati esterni.

2. Il ReGIndE censisce i soggetti abilitati esterni che intendono fruire dei servizi telematici di cui al presente regolamento.

3. I sistemi di gestione informatizzata dei registri di cancelleria utilizzano il ReGIndE al fine di evitare l'inserimento manuale dei dati.

4. Le categorie di soggetti (nel prosieguo anche enti) il cui profilo anagrafico alimenta il ReGIndE sono:

a) soggetti rappresentanti un ente pubblico o privato, chiamati a svolgere una specifica attività processuale nell'ambito di procedimenti civili o penali, escluse le parti private;

b) professionisti iscritti in albi ed elenchi istituiti con legge;

c) professionisti non iscritti ad alcun albo: tutti i soggetti nominati dal giudice come consulenti tecnici d'ufficio, periti o più in generale ausiliari del giudice, non appartenenti ad un ordine di categoria o che appartengono ad ente/ordine professionale che non abbia ancora inviato l'albo al Ministero della giustizia (ad eccezione degli avvocati).

5. Il ReGIndE è direttamente accessibile dai sistemi interni al dominio giustizia, attraverso un apposito web service.

6. Il ReGIndE è consultabile dai soggetti abilitati esterni tramite il proprio punto di accesso o tramite il PST, su connessioni sicure (SSL v3), attraverso un apposito web service; i relativi WSDL sono pubblicati nell'area pubblica del PST.

Articolo 8

(Alimentazione del registro generale degli indirizzi elettronici)

1. L'alimentazione del ReGIndE avviene previo invio al responsabile per i sistemi informativi automatizzati di un documento di censimento contenente le informazioni necessarie ad identificare:

a) l'ente stesso attraverso: codice ente, descrizione, codice fiscale/partita iva;

b) il nominativo e il codice fiscale del delegato all'invio dell'albo, che dovrà sottoscrivere con firma digitale o firma elettronica qualificata l'albo in trasmissione;

c) la casella di PEC utilizzata per l'invio dell'albo.

2. Il documento di censimento di cui al comma precedente aderisce al modello reperibile nell'area pubblica del portale e viene inviato all'indirizzo di posta elettronica certificata del responsabile per i sistemi informativi automatizzati: prot.dgsia.ddsc@giustiziacert.it.

3. Terminate le operazioni di censimento da parte del responsabile per i sistemi informativi automatizzati, l'ente mittente del documento di censimento riceve una risposta; in caso di esito positivo, l'ente può procedere all'invio dell'albo secondo le seguenti specifiche:

a) il messaggio deve essere di posta elettronica certificata; non sono considerati i messaggi di posta ordinaria;

b) non vi sono vincoli sull'oggetto né sul corpo del messaggio;

c) l'indirizzo di PEC mittente deve essere censito tra quelli delegati all'invio e riportati nel documento di censimento;

d) deve essere allegato un solo file (ComunicazioniSoggetti.xml sottoscritto con firma digitale o firma elettronica qualificata;

e) la firma digitale o firma elettronica qualificata deve appartenere al soggetto delegato di cui al comma 1, lettera b, sulla base del codice fiscale censito;

f) il file ComunicazioniSoggetti.xml deve essere conforme all'XML-Schema di cui all'Allegato 2;

g) il codice ente specificato nel file deve essere tra quelli censiti.

4. Il mancato rispetto di uno o più dei vincoli di cui all'articolo precedente comporta un messaggio automatico di esito negativo; in questo caso l'allegato ComunicazioniSoggetti.xml viene scartato.

5. A ogni invio corrisponde una risposta tramite PEC; il messaggio ha come oggetto la medesima descrizione del messaggio originale con il suffisso "– Esito" e riporta in allegato l'esito dell'elaborazione del messaggio con le eventuali eccezioni; il formato del messaggio di esito, inviato come allegato al messaggio di PEC, è descritto nell'Allegato 3.

6. L'esito si riferisce sia ad errori presenti sui dati e, quindi riconducibili alle informazioni dei singoli soggetti (come, ad esempio, codice fiscale inesistente), sia ad errori legati a vincoli e

prerequisiti che presuppongono la validità dell'invio di un albo (ad esempio: censimento dell'ente richiedente e dei soggetti abilitati all'invio dell'albo).

7. Ad ogni nuovo indirizzo di PEC registrato nelle anagrafiche a seguito dell'inserimento di un nuovo soggetto o di modifica di uno esistente, viene inviato un messaggio di PEC di cortesia in cui si attesta l'avvenuta registrazione.

Articolo 9

(Professionisti non iscritti in albi)

1. I professionisti non iscritti all'albo, oppure per i quali il proprio ordine di appartenenza non abbia provveduto all'invio di copia dell'albo (ad eccezione degli avvocati), si registrano al ReGIndE attraverso un PdA o attraverso il PST, previa identificazione, effettuando altresì l'inserimento (upload) del file che contiene copia informatica, in formato PDF, dell'incarico di nomina da parte del giudice; tale file è sottoscritto con firma digitale o firma elettronica qualificata dal soggetto che intende iscriversi.

2. Il PdA provvede a trasmettere l'avvenuta registrazione con le medesime modalità di cui all'articolo precedente, con la differenza che il file ComunicazioniSoggetti.xml è digitalmente sottoscritto con firma digitale o firma elettronica qualificata dal PdA.

3. Qualora il professionista di cui al comma 1 s'iscriva ad un albo, oppure pervenga copia dell'albo da parte dell'ordine di appartenenza, prevalgono i dati trasmessi dall'ordine stesso; in questo caso il sistema cancella la prima iscrizione e invia un messaggio PEC di cortesia al professionista.

Articolo 10

(Indirizzi PEC delle pubbliche amministrazioni e degli enti privati)

1. La pubblica amministrazione o l'ente privato che deve comunicare il proprio indirizzo di posta elettronica certificata per la ricezione delle comunicazioni e notificazioni, ai sensi dell'articolo 16, comma 12, primo periodo, del decreto-legge 18 ottobre 2012, n. 179, convertito con modificazioni nella legge 17 dicembre 2012, n. 221, procede inserendo tale indirizzo sul PST.

2. Ai fini di cui al comma precedente, l'amministrazione pubblica o l'ente privato invia all'indirizzo di posta elettronica certificata della DGSIA (prot.dgsia.ddsc@giustiziacert.it) un documento aderente allo specifico modello disponibile nell'area pubblica del PST, contenente le seguenti informazioni:

a) denominazione e codice fiscale della amministrazione pubblica o dell'ente privato;

b) nominativo e codice fiscale del soggetto incaricato di inserire o modificare l'indirizzo di PEC dell'amministrazione pubblica sul PST;

c) denominazione e codice fiscale o, in mancanza, il codice IPA dei propri organi o articolazioni, anche territoriali, presso cui eseguire le comunicazioni e notificazioni per via telematica nel caso in cui sia stabilito presso questi l'obbligo di notifica degli atti introduttivi di giudizio in relazione a specifiche materie ovvero in caso di autonoma capacità o legittimazione processuale; in mancanza di codice fiscale o di codice IPA si provvederà ai sensi dell'articolo 11, comma 2, lett. a);

d) denominazione e codice fiscale o, in mancanza, il codice IPA delle specifiche aree organizzative omogenee presso cui l'amministrazione pubblica elegge domicilio ai fini del giudizio; in mancanza di codice fiscale o di codice IPA si provvederà ai sensi dell'articolo 11, comma 2, lett. a).

3. Il soggetto incaricato di cui alla lettera b) del comma precedente accede ad un'apposita area riservata del PST, previa identificazione informatica, secondo le specifiche di cui all'articolo 6, e inserisce o modifica:

a) l'indirizzo di PEC della pubblica amministrazione o dell'ente privato;

b) il nominativo, il codice fiscale e l'indirizzo di PEC di eventuali dipendenti o rappresentanti, tramite i quali la pubblica amministrazione o l'ente privato stanno in giudizio personalmente o svolgono attività processuale consentita; tali soggetti alimentano il ReGIndE.

4. Inserito o modificato l'indirizzo di PEC di cui al comma precedente, il soggetto incaricato inserisce o modifica il nominativo, il codice fiscale e l'indirizzo di PEC di eventuali dipendenti o rappresentanti tramite i quali la pubblica amministrazione o l'ente privato sta in giudizio personalmente o svolge attività processuale consentita; tali soggetti alimentano il ReGIndE.

5. Per le amministrazioni pubbliche il cui indirizzo di PEC sia già censito ai sensi dell'articolo 16, comma 12, primo periodo, del decreto-legge 18 ottobre 2012, n. 179, convertito con modificazioni nella legge 17 dicembre 2012, n. 221, la comunicazione dei dati di cui alle lettere c) e d) del comma 2 e delle loro successive modificazioni avviene mediante l'invio di un documento, aderente allo specifico modello reperibile sull'area pubblica del PST, al medesimo indirizzo di posta elettronica certificata della DGSIA indicato al comma 2.

6. L'elenco degli indirizzi di PEC delle pubbliche amministrazioni e degli enti privati è consultabile dagli uffici giudiziari e dagli UNEP attraverso i sistemi informatici a disposizione dei soggetti abilitati interni.

7. L'elenco degli indirizzi di PEC di cui al comma 3, è consultabile dagli avvocati tramite il proprio punto di accesso o tramite il PST (area riservata), su connessioni sicure, attraverso un apposito web service, che verifica la presenza dell'avvocato sul ReGIndE; i relativi WSDL sono pubblicati nell'area pubblica del PST. L'accesso è tracciato in appositi log, che il Ministero della giustizia conserva per cinque anni, recanti: il punto di accesso attraverso cui è stato effettuato l'accesso, la data e l'ora dell'accesso.

Articolo 11

(Indirizzi PEC degli organi, articolazioni e aree organizzative omogenee delle pubbliche amministrazioni)

1. Effettuate dall'incaricato dell'amministrazione pubblica le attività previste dal comma 3 dell'articolo 10, gli organi, le articolazioni, anche territoriali, e le aree organizzative omogene (AOO), indicate nel documento di cui al comma 2 dell'articolo 10, comunicano il proprio indirizzo di posta elettronica certificata per la ricezione delle comunicazioni e notificazioni.

2. Ai fini del comma precedente, ciascun organo, articolazione, anche territoriale, o area organizzativa omogenea (AOO) invia all'indirizzo di posta elettronica certificata della DGSIA (prot.dgsia.ddsc@giustiziacert.it) un documento di censimento, aderente al modello reperibile nell'area pubblica del PST, contenente le seguenti informazioni:

a) denominazione e codice fiscale dell'amministrazione pubblica di cui al comma 1 ed il codice fiscale dell'organo, dell'articolazione, anche territoriale, o dell'area organizzativa omogenea stessa

o, in mancanza, il relativo codice IPA. In difetto di codice fiscale o di codice IPA, la DGSIA assegnerà un codice identificativo univoco che sarà reso noto nella comunicazione di avvenuto censimento e che, unitamente al codice fiscale dell'amministrazione pubblica di cui al comma 1, dovrà essere indicato per la costituzione in giudizio e per i depositi telematici;

b) nominativo e codice fiscale del soggetto incaricato di inserire o modificare gli indirizzi di PEC dell'organo, dell'articolazione o della AOO sul PST.

3. Il soggetto incaricato di cui alla lettera b) del comma precedente accede ad un'apposita area riservata del PST, previa identificazione autenticazione informatica, secondo le specifiche di cui all'articolo 6, e inserisce o modifica l'indirizzo di PEC dell'organo, dell'articolazione, anche territoriale, o della AOO.

4. Effettuate le attività di cui al comma che precede, il soggetto incaricato inserisce o modifica il nominativo, il codice fiscale e l'indirizzo di PEC di eventuali dipendenti tramite i quali l'organo, l'articolazione, anche territoriale, o l'area organizzativa omogenea sta in giudizio personalmente; tali soggetti alimentano il ReGIndE.

5. L'elenco degli indirizzi di PEC degli organi e delle articolazioni, anche territoriali, nonché la speciale sezione dell'elenco contenente gli indirizzi PEC delle aree organizzative omogenee (AOO) delle amministrazioni pubbliche sono consultabili dagli uffici giudiziari e dagli UNEP attraverso i sistemi informatici a disposizione dei soggetti abilitati interni e dagli avvocati secondo le medesime modalità previste dal comma 5 dell'articolo 10.

Articolo 12

(Sistemi informatici per i soggetti abilitati interni)

1. I sistemi informatici a disposizione dei soggetti abilitati interni sono conformi alle regole di cui al decreto del Ministro della giustizia 27 aprile 2009 e mettono a disposizione le funzioni relative a:

a) ricezione, accettazione e trasmissione dei dati e dei documenti informatici;

b) consultazione e gestione del fascicolo informatico.

2. Per l'accesso ai sistemi di cui al comma precedente dall'interno degli uffici giudiziari, l'identificazione è effettuata mediante coppia di credenziali "nome utente/password" oppure mediante autenticazione a due fattori.

3. Per l'accesso ai sistemi di cui al comma 1 dall'esterno della Rete Giustizia, l'identificazione è effettuata dal PST sulla base del sistema "Active Directory Nazionale" (ADN) tramite autenticazione a due fattori; ai soli fini del recupero dall'esterno delle informazioni di registro da parte dei sistemi a disposizione dei magistrati in ambito civile, è sufficiente l'identificazione sulla base del sistema ADN purché l'interrogazione dei dati finalizzati al recupero preveda l'indicazione del numero di ruolo generale nonché del codice fiscale dell'attore principale e del convenuto principale del procedimento.

Articolo. 13

(Fascicolo informatico)

1. Il fascicolo informatico raccoglie i documenti (atti, allegati, ricevute di posta elettronica certificata) da chiunque formati, nonché le copie informatiche dei documenti; raccoglie altresì le copie informatiche dei medesimi atti quando siano stati depositati su supporto cartaceo.

2. Il sistema di gestione del fascicolo informatico, realizzato secondo quanto previsto all'articolo 41 del CAD, è la parte del sistema documentale del Ministero della giustizia che si occupa di archiviare e reperire tutti i documenti informatici, prodotti sia all'interno che all'esterno; fornisce pertanto ai sistemi fruitori (sistemi di gestione dei registri di cancelleria, gestore dei servizi telematici e strumenti a disposizione dei magistrati) tutti i metodi – esposti attraverso appositi web service – necessari per il recupero, l'archiviazione e la conservazione dei documenti informatici, secondo la normativa in vigore; l'accesso al sistema di gestione documentale avviene soltanto per il tramite dei sistemi fruitori, che gestiscono le logiche di profilazione e autorizzazione.

3. Le operazioni di accesso al fascicolo informatico sono registrate in un apposito file di log che contiene le seguenti informazioni:

a) il codice fiscale del soggetto che ha effettuato l'accesso;

b) il riferimento al documento prelevato o consultato (codice identificativo del documento nell'ambito del sistema documentale);

c) la data e l'ora dell'accesso.

4. Il suddetto file di log è sottoposto a procedura di conservazione, sempre nell'ambito del sistema documentale, per cinque anni.

CAPO III

TRASMISSIONE DI ATTI E DOCUMENTI INFORMATICI

Articolo 14

(Formato dell'atto del procedimento in forma di documento informatico)

1. L'atto del procedimento civile o penale in forma di documento informatico, da depositare telematicamente nell'ufficio giudiziario, deve rispettare i seguenti requisiti:

a) è in formato PDF o PDF/A;

b) è privo di elementi attivi;

c) è ottenuto dalla trasformazione di un documento testuale, senza restrizioni per le operazioni di selezione e copia di parti; non è pertanto ammessa la scansione di immagini;

d) è sottoscritto con firma digitale o firma elettronica qualificata esterna secondo la struttura riportata ai commi seguenti;

e) è privo di protezione di password;

f) nel procedimento civile è corredato da un file in formato XML, che contiene le informazioni strutturate nonché tutte le informazioni della nota di iscrizione a ruolo, e che rispetta gli XSD riportati nell'Allegato 5; esso è denominato DatiAtto.xml ed è sottoscritto con firma digitale o firma elettronica qualificata.

2. La struttura del documento firmato è PAdES-BES (o PAdES Part 3) o CAdES-BES; il certificato di firma è inserito nella busta crittografica; è fatto divieto di inserire nella busta crittografica le informazioni di revoca riguardanti il certificato del firmatario. La modalità di apposizione della firma digitale o della firma elettronica qualificata è del tipo "firme multiple indipendenti" o parallele, e prevede che uno o più soggetti firmino, ognuno con la propria chiave

privata, lo stesso documento (o contenuto della busta). L'ordine di apposizione delle firme dei firmatari non è significativo e un'alterazione dell'ordinamento delle firme non pregiudica la validità della busta crittografica; nel caso del formato CAdES il file generato si presenta con un'unica estensione p7m. Il meccanismo qui descritto è valido sia per l'apposizione di una firma singola che per l'apposizione di firme multiple.

3. Le applicazioni di generazione della firma digitale o qualificata per la sottoscrizione dei documenti informatici devono utilizzare la funzione di hash di cui all'art 4, comma 2, del Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013.

Articolo 15

(Formato dei documenti informatici allegati)

1. I documenti informatici allegati, compresa la procura alle liti rilasciata su supporto analogico, sono privi di elementi attivi, tra cui macro e campi variabili, e sono consentiti nei seguenti formati:

a) documenti impaginati - PDF o PDF/A (.pdf), con dimensioni cm 21,00 per 29,70 (formato A4), Rich-Text Format (.rtf).

b) Immagini raster - JPEG (.jpg, .jpeg), TIFF (.tif, .tiff), GIF (.gif).

c) Video - formati video delle famiglie MPEG2 e MPEG4 (.mp4, .m4v, .mov, .mpg, .mpeg), AVI (.avi).

d) Suono: MP3 (.mp3), FLAC (.flac), audio RAW (.raw), Waveform Audio File Format (.wav), AIFF (.aiff, .aif).

e) Testo - TXT (.txt).

f) Ipertesto – XML Extended markup language (.xml).

g) Posta elettronica - eml (.eml), purché contenenti file nei formati di cui alle lettere precedenti (a-f)

h) Posta elettronica - .msg, purché contenenti file nei formati di cui alle lettere da a) a g).

i) Formato compresso: è consentito l'utilizzo dei seguenti formati compressi purché contenenti file nei formati previsti alle lettere precedenti: .zip, .rar, .arj.

2. Gli allegati sono sottoscritti con firma digitale o firma elettronica qualificata nei casi previsti dalla legge. Nel caso di formati compressi la firma digitale, se presente, deve essere applicata dopo la compressione.

Articolo 16

(Trasmissione di atti da parte dei soggetti abilitati esterni nel procedimento civile)

1. Nel procedimento civile l'atto in forma di documento informatico e gli allegati di cui all'articolo 15, sono trasmessi dai soggetti abitati esterni mediante la posta elettronica certificata di cui al d.p.r. 11 febbraio 2005, n. 68.

2. L'atto e gli allegati sono contenuti nella cosiddetta "busta telematica", ossia un file in formato MIME che riporta tutti i dati necessari per l'elaborazione da parte del sistema ricevente (gestore dei servizi telematici); in particolare la busta contiene il file Atto.enc, ottenuto dalla cifratura del file Atto.msg, il quale contiene a sua volta:

a) IndiceBusta.xml: il DTD è riportato nell'Allegato 4. Tale file deve essere omesso qualora il suo contenuto sia presente nella sezione apposita del file DatiAtto.xml, come da XSD di cui al successivo punto b).;

b) DatiAtto.xml: gli XSD sono riportati nell'Allegato 5;

c) <nome file (libero)>: atto vero e proprio, in formato PDF o PDF/A, sottoscritto con firma digitale o firma elettronica qualificata secondo la struttura dell'articolo 16 comma 2;

d) AllegatoX.xxx: uno o più allegati nei formati di file di cui all'articolo 17, eventualmente sottoscritti con firma digitale o firma elettronica qualificata; il nome del file può essere scelto liberamente.

3. La cifratura di Atto.msg è eseguita con la chiave di sessione (ChiaveSessione) cifrata con il certificato del destinatario; IssuerDname è il Distinguished Name della CA che ha emesso il certificato dell'ufficio giudiziario o dell'UNEP destinatario, SerialNumber è il numero seriale del certificato dell'ufficio giudiziario o dell'UNEP destinatario; l'algoritmo utilizzato per l'operazione di cifratura simmetrica del file è il 3DES e le chiavi simmetriche di sessione sono cifrate utilizzando la chiave pubblica contenuta nel certificato del destinatario; le chiavi di cifratura degli uffici giudiziari sono disponibili nell'area pubblica del PST (il relativo percorso e nome file è indicato nel catalogo dei servizi telematici).

4. La dimensione massima consentita per la busta telematica è pari a 60 Megabyte.

5. La busta telematica viene trasmessa all'ufficio giudiziario destinatario in allegato ad un messaggio di posta elettronica certificata che rispetta le specifiche su mittente, destinatario, oggetto, corpo e allegati come riportate nell'Allegato 6.

6. Il gestore dei servizi telematici scarica il messaggio dal gestore della posta elettronica certificata del Ministero della giustizia ed effettua le verifiche formali sul messaggio; le eccezioni gestite sono le seguenti:

a) T001: l'indirizzo del mittente non è censito in ReGIndE;

b) T002: Il formato del messaggio non è aderente alle specifiche;

c) T003: la dimensione del messaggio eccede la dimensione massima consentita.

7. Il gestore dei servizi telematici, nel caso in cui il mittente sia un avvocato, effettua l'operazione di certificazione, ossia recupera lo status del difensore da ReGIndE; nel caso in cui lo status non sia "attivo", viene segnalato alla cancelleria.

8. Il gestore dei servizi telematici effettua i controlli automatici (formali) sulla busta telematica; le possibili anomalie all'esito dell'elaborazione della busta telematica sono codificate secondo le seguenti tipologie:

a) WARN (WARNING): anomalia non bloccante; si tratta in sostanza di segnalazioni, tipicamente di carattere giuridico (ad esempio manca la procura alle liti allegata all'atto introduttivo certificato di firma non valido o mittente non firmatario dell'atto);

b) ERROR: anomalia bloccante che si verifica in tutti i casi nei quali è necessario o opportuno un intervento della cancelleria al fine di consentire l'accettazione dell'atto;

c) FATAL: anomalia bloccante, eccezione non gestita o non gestibile (esempio: impossibile decifrare la busta depositata o elementi della busta mancanti ma fondamentali per l'elaborazione).

9. La codifica puntuale degli errori indicati al comma precedente è pubblicata e aggiornata nell'area pubblica del PST.

10. In caso di anomalia bloccante (FATAL) il gestore dei servizi telematici invia al depositante un messaggio di posta elettronica certificata, contenente il rifiuto da parte del cancelliere o del segretario.

11. La busta telematica è conservata nel sistema documentale di cui all'articolo 13, comma 2.

12. L'accettazione automatica sarà efficace a decorrere dalla pubblicazione del provvedimento del Direttore generale SIA, adottato all'esito dell'avvenuta verifica dell'adeguamento dei sistemi.

Articolo 17

(Trasmissione di atti attraverso il portale delle notizie di reato)

1. La trasmissione di atti e di documenti in modalità telematica agli uffici del pubblico ministero presso i tribunali ordinari, da parte degli ufficiali e degli agenti di polizia giudiziaria e di ogni altro soggetto tenuto per legge alla trasmissione della notizia di reato, avviene attraverso il PNR, accessibile all'indirizzo: https://portalendr.giustizia.it/NdrWEB/home.do.

2. L'abilitazione dei referenti interni agli uffici del pubblico ministero avviene tramite la procedura di seguito descritta:

a) il procuratore della Repubblica individua uno o più referenti interni per il PNR e ne comunica le generalità alla DGSIA a mezzo protocollo;
b) il referente dell'ufficio del pubblico ministero si accredita tramite l'applicativo RAFE richiedendo il certificato alla DGSIA;
c) attraverso lo stesso applicativo la DGSIA verifica e approva la richiesta, inviando al referente una comunicazione di posta elettronica che contiene il Certificato per l'accesso a RAFE;
d) il referente dell'ufficio del pubblico ministero, con l'applicativo RAFE, gestisce la distribuzione dei Certificati ai referenti degli uffici fonte.

3. L'abilitazione dei referenti del PNR degli uffici fonte avviene tramite la procedura di seguito descritta:

a) l'Ufficio Fonte individua uno o più referenti e ne comunica le generalità all'ufficio del pubblico ministero del circondario di riferimento;
b) il referente dell'Ufficio Fonte, tramite l'applicativo RAFE, richiede il certificato all'ufficio del pubblico ministero a cui sono state inviate le proprie generalità;
c) con lo stesso applicativo il referente dell'ufficio del pubblico ministero destinatario della richiesta la approva e la invia al richiedente una comunicazione di posta elettronica contenente il Certificato di accesso a RAFE.

4. L'abilitazione degli operatori degli uffici fonte avviene tramite la procedura di seguito descritta:

a) il referente dell'Ufficio Fonte, con l'applicativo RA.FE., gestisce la distribuzione dei Certificati agli operatori del proprio ufficio;
b) il referente dell'Ufficio Fonte, con l'applicativo RA.FE., genera un Certificato per ogni operatore del proprio ufficio ed invia loro una comunicazione di posta elettronica contenente il predetto Certificato;
c) l'operatore accede al PNR col proprio certificato ed è abilitato all'invio delle comunicazioni di atti e di documenti in modalità telematica agli uffici del pubblico ministero.

5. Il Certificato emesso è nominativo e consente l'accesso all'applicativo per cui è stato generato. Il Certificato deve essere installato sulla postazione di lavoro ed ha una validità di due anni dal

momento della emissione. Il Certificato può essere revocato, impedendo all'utente titolare di accedere all'applicativo.

6. L'atto in forma di documento informatico contenente la comunicazione della notizia di reato e gli atti contenenti le note informative successive, rispettano i seguenti requisiti:

a) sono in formato PDF;
b) sono ottenuti da una trasformazione di un documento testuale, senza restrizioni per le operazioni di selezione e copia di parti; non è pertanto ammessa la scansione di immagini;
c) sono sottoscritti con firma digitale o firma elettronica qualificata.

7. Gli allegati, in forma di documento informatico, rispettano i seguenti requisiti:

a) sono in formato PDF;
b) possono essere sottoscritti con firma digitale o firma elettronica qualificata.

8. Gli atti e gli allegati di cui ai commi 6 e 7 possono avere una dimensione massima complessiva di 30 Megabyte.

9. Le tipologie di firma ammesse sono CAdES e PAdES.

10. Gli atti e gli allegati sono trasmessi secondo la procedura del PNR che consiste:

a) nell'inserimento dei dati richiesti dal sistema;
b) nel caricamento dell'atto contenente la notizia di reato o la nota informativa successiva ed i relativi allegati;
c) nell'esecuzione del comando di invio.

11. Il PNR consente di salvare i dati ed i documenti caricati per un successivo invio. I dati ed i documenti restano disponibili per un successivo invio per sessanta giorni dal primo salvataggio in bozza, decorsi i quali verranno automaticamente cancellati. Il PNR dà evidenza all'operatore dell'ufficio fonte del decorso dei primi trenta giorni.

12. Il PNR genera la ricevuta di accettazione nel momento in cui la comunicazione diviene disponibile nelle "Annotazioni Preliminari dal Portale". La ricevuta di accettazione, che è scaricabile e resta a disposizione dell'operatore dell'ufficio fonte sul PNR, contiene:

a) data e orario in cui la comunicazione diviene disponibile nelle "Annotazioni Preliminari dal Portale";
b) tipologia notizia di reato;
c) ufficio Fonte;
d) ufficio del pubblico ministero destinatario;
e) numero protocollo PNR;
f) numero protocollo "Annotazioni Preliminari dal Portale".

13. Il PNR consente, in caso di urgenza, la comunicazione di notizie di reato selezionando l'apposita funzione. Una notizia di reato urgente viene selezionata con priorità maggiore per l'invio rispetto ad una ordinaria.

14. L'operatore dell'ufficio fonte può visualizzare lo stato della comunicazione, così come definito di seguito:

a) ATTESA DI INVIO: presa in carico dal sistema;
b) INVIATA: In transito;
c) ACQUISITA: Comunicazione nella disponibilità dell'ufficio del pubblico ministero destinatario nelle "Annotazioni preliminari da Portale" (primo invio);
d) RIGETTATA: La segreteria dell'ufficio del pubblico ministero non ha convalidato i dati e/o gli allegati della notizia di reato;

e) RIACQUISITA: Comunicazione nuovamente nella disponibilità dell'ufficio del pubblico ministero destinatario nelle "Annotazioni preliminari da Portale" (dopo un rigetto da parte dell'ufficio del pubblico ministero);
f) PROTOCOLLATA: Iscritta nel registro/inserita nel fascicolo come nota informativa successiva.

15. Gli atti e i documenti, nonché gli allegati, correttamente acquisiti da Re.Ge.WEB sono visibili unicamente dal personale di segreteria abilitato dal procuratore della Repubblica all'accesso alle "Annotazioni Preliminari dal Portale", secondo gli stati delle comunicazioni individuati di seguito:

a) ACQUISITA: Nella disponibilità dell'ufficio del pubblico ministero destinatario (primo invio);
b) RIGETTATA: L'ufficio del pubblico ministero non ha convalidato i dati e/o gli allegati della notizia di reato;
c) RIACQUISITA: Nuovamente nella disponibilità dell'ufficio del pubblico ministero (dopo un rigetto).

16. Le trasmissioni utilizzano algoritmi di cifratura asimmetrica e chiavi di sessione con le seguenti caratteristiche:

a) chiave di sessione a 256 bit per cifrare gli atti, i documenti e gli allegati con AES;
b) la chiave di sessione viene cifrata con una chiave asimmetrica RSA a 2048 bit. I dati personali, una volta che la comunicazione assume lo stato "Acquisita" di cui al comma 12 non sono più presenti sul PNR.

Articolo 18

(Trasmissione di atti da parte dei soggetti abilitati esterni nel procedimento penale)

1. Nel procedimento penale l'atto in forma di documento informatico e gli allegati di cui all'articolo 16, sono trasmessi dai soggetti abitati esterni mediante il PDP, accessibile dal PST all'indirizzo https://pst.giustizia.it, tramite l'area riservata di cui all'articolo 5.

2. L'identificazione informatica dei difensori per l'accesso all'area riservata avviene mediante SPID o smart card.

3. L'accesso al PDP è consentito unicamente ai soggetti iscritti nel ReGIndE con ruolo avvocato, praticante abilitato, nonché avvocato ente pubblico e funzionario ente pubblico, questi ultimi limitatamente agli appartenenti all'Avvocatura dello Stato.

4. Le trasmissioni utilizzano algoritmi di cifratura asimmetrica e chiavi di sessione conformi a quanto previsto dall'articolo 16, comma 2.

5. L'atto principale è ammesso quando rispetta i requisiti di cui all'articolo 16, comma 1, lettere da a) ad e). È consentita la scansione di documento analogico purché in bianco e nero e con una risoluzione pari a 200 dpi.

6. Alla trasmissione dell'atto di nomina nella procura della Repubblica deve essere allegato un atto abilitante, quando il procedimento sia in fase di indagine preliminare e non sia stato ancora emesso o non sia previsto uno degli avvisi di cui agli articoli 408, 411 o 415 bis codice di procedura penale.

7. La preventiva annotazione nel ReGeWEB, a cura delle cancellerie e segreterie degli uffici giudiziari, del codice fiscale dei soggetti abilitati esterni è requisito indispensabile per ottenere la visibilità dei procedimenti autorizzati.

8. La procedura di trasmissione tramite il PDP consiste:

a) nell'inserimento dei dati richiesti dal sistema;

b) nel caricamento dell'atto del procedimento e dei documenti allegati;

c) nell'esecuzione del comando di invio.

9. Il PDP, al termine della procedura di cui ai commi precedenti genera la ricevuta di accettazione del deposito (art. 172 c.p.p.) che contiene:

a) un identificativo unico nazionale nella forma anno/numero;

b) i dati inseriti dal depositante;

c) la data e l'orario dell'operazione di invio rilevati dai sistemi del Ministero di Giustizia.

10. La ricevuta è scaricabile in formato PDF e resta, comunque, a disposizione del difensore sul PDP.

11. A seguito dell'invio dell'atto processuale i sistemi informativi ministeriali procedono alla verifica ed accettazione automatica del deposito degli atti inviati dai difensori rispetto ai quali vi è corrispondenza tra i dati inseriti sul PDP ed i dati di registro del procedimento penale, senza intervento degli operatori di segreteria e di cancelleria.

12. Il difensore può verificare lo stato del deposito accedendo al PDP nella sezione "Consultazione - Depositi"

13. Il personale amministrativo degli uffici giudiziari ha a disposizione apposite funzionalità per la gestione dei depositi pervenuti tramite il PDP e si avvale dell'ausilio dell'esito dei preventivi controlli automatici eseguiti dai sistemi.

14. All'accettazione o al rigetto del deposito gli atti del procedimento ed i documenti allegati in forma di documento informatico sono conservati nel sistema documentale di cui all'articolo 13, comma 2.

15. I possibili valori di stato del deposito sul PDP sono:

a) INVIATO: eseguita con successo l'operazione di "Invio";
b) IN TRANSITO: in attesa di smistamento al sistema informativo dell'ufficio giudiziario destinatario; nel momento in cui il deposito assume lo stato "in transito", il PDP cancella tutti i dati personali;
c) ACCETTATO (automaticamente o a seguito di verifiche ove previste): intervenuta associazione dell'atto inviato al procedimento di riferimento. L'associazione è automatica nel caso di coincidenza tra i dati inseriti sul PDP ed i dati di registro del procedimento penale e, quando previsto, in presenza dell'atto abilitante di cui all'articolo 17 comma 2. L'associazione è ad opera del cancelliere o del segretario qualora, dopo le verifiche, sia stato individuato univocamente il procedimento di riferimento. Nel caso di denuncia, di querela e di istanza di procedimento, l'accoglimento equivale al ricevimento ed iscrizione del procedimento nel ReGeWEB da parte della procura della Repubblica;
d) IN VERIFICA: anomalia bloccante, il deposito è pervenuto nel sistema dell'ufficio giudiziario destinatario ma non essendoci coincidenza di dati non è stato automaticamente associato ad un procedimento ed è sottoposto a verifiche da parte del personale dell'ufficio;
e) RIFIUTATO: anomalia bloccante; rifiuto del deposito successivo alle verifiche automatiche e ad opera del personale dell'ufficio; la motivazione è riportata sul PDP;
f) ERRORE TECNICO: anomalia bloccante; si è verificato un problema in fase di trasmissione; il difensore è invitato dal messaggio di stato del PDP ad effettuare nuovamente il deposito.

16. Il difensore può consultare tutti gli stati del deposito accedendo alla relativa sezione del PDP, e scaricare un documento che attesta gli esiti: accolto, rigettato ed errore tecnico. Tali esiti sono altresì

comunicati a mezzo mail ordinaria, previa configurazione della stessa da parte del difensore nella sezione “Preferenze” del PDP.

17. La dimensione massima consentita per ciascun deposito di atti ed eventuali allegati è pari a 60 Megabyte per singolo file, fino ad un massimo di 600 Megabyte per l’intero deposito.

18. L'accettazione automatica di cui al comma 15, lett. c), sarà efficace a decorrere dalla pubblicazione del provvedimento del Direttore generale SIA, adottato all’esito dell’avvenuta verifica dell'adeguamento dei sistemi.

Articolo 19

(Trasmissione di atti da parte dei soggetti abilitati interni)

1. Nei procedimenti civili e penali i soggetti abilitati interni utilizzano appositi strumenti per la redazione degli atti del processo in forma di documento informatico e per la loro trasmissione alla cancelleria o alla segreteria dell’ufficio giudiziario.

2. Nel procedimento civile l’atto è inserito nella medesima busta telematica di cui all’articolo 18 e viene trasmesso su canale sicuro (SSL v3) al gestore dei servizi telematici, tramite collegamento sincrono (http/SOAP); si applicano le disposizioni di cui all’articolo 18, comma 2.

3. Se il provvedimento del magistrato è redatto in forma di documento analogico~~,~~ il cancelliere o il segretario dell’ufficio giudiziario ne estrae copia in formato PDF e lo inserisce nel fascicolo informatico.

Articolo 20

(Comunicazioni e notificazioni per via telematica)

1. Il gestore dei servizi telematici provvede ad inviare le comunicazioni o le notificazioni per via telematica, provenienti dall’ufficio giudiziario, alla casella di posta elettronica certificata del soggetto abilitato esterno o dell’utente privato destinatario, recuperando il relativo indirizzo dai pubblici elenchi di cui agli articoli 6-bis, 6-ter e 6-quater del CAD; il formato del messaggio è riportato nell’Allegato 8; la comunicazione o notificazione è riportata nel corpo del messaggio nonché nel file allegato Comunicazione.xml (il relativo DTD è riportato nell’Allegato 4).

2. La cancelleria o la segreteria dell’ufficio giudiziario, attraverso apposite funzioni messe a disposizione dai sistemi informatici di cui all’articolo 12, provvede ad effettuare una copia per immagine in formato PDF di eventuali documenti cartacei da comunicare; la copia informatica è conservata nel fascicolo informatico.

3. Il gestore dei servizi telematici recupera le ricevute della posta elettronica certificata e gli avvisi di mancata consegna dal gestore di PEC del Ministero e li conserva nel fascicolo informatico; la ricevuta di avvenuta consegna è di tipo breve per le comunicazioni e di tipo completo per le notificazioni.

Articolo 21

(Comunicazioni e notificazioni contenenti dati sensibili)

1. La comunicazione o la notificazione che contiene dati sensibili è effettuata per estratto; in questo caso al destinatario viene recapitato l’avviso di disponibilità, secondo il formato riportato

nell'Allegato 8; il destinatario effettua il prelievo dell'atto integrale accedendo all'indirizzo (URL) contenuto nel suddetto messaggio di PEC di avviso.

2. Il prelievo di cui al comma precedente avviene attraverso l'apposito servizio proxy del PST, su canale sicuro (protocollo SSL); tale servizio effettua l'identificazione informatica dell'utente, ai sensi dell'articolo 6; il prelievo è consentito unicamente se l'utente è registrato nel ReGIndE.

3. Il prelievo di cui al comma precedente avviene da un'apposita area di download del gestore dei servizi telematici, dove viene gestita e mantenuta un'apposita tabella recante le seguenti informazioni:

a) il codice fiscale del soggetto che ha effettuato il prelievo o la consultazione;

b) il riferimento al documento prelevato o consultato (codice univoco inserito nell'URL inviato nell'avviso di cui al comma 4);

c) la data e l'ora di invio dell'avviso;

d) la data e l'ora del prelievo o della consultazione.

4. Le informazioni di cui al comma precedente vengono conservate per cinque anni.

5. Nel caso in cui il destinatario sia un'impresa iscritta nel relativo registro o una Pubblica Amministrazione, la comunicazione o la notificazione che contiene dati sensibili è effettuata ai sensi del comma 1; l'utente che accede all'indirizzo (URL) contenuto nel messaggio di PEC di avviso, su canale sicuro (protocollo SSL), viene identificato ai sensi dell'art 6 ed è abilitato ad accedere all'atto integrale solo se appartiene all'impresa destinataria come risultante dal registro delle imprese o se è un dipendente della Pubblica Amministrazione autorizzato.

Articolo 22

(Notificazioni per via telematica a cura degli UNEP)

1. Le richieste telematiche di un'attività di notificazione da parte di un ufficio giudiziario sono inoltrate al sistema informatico dell'UNEP in formato XML, attraverso un colloquio diretto, via web service, tra i rispettivi gestori dei servizi telematici, su canale sicuro (SSL v3), oppure tramite posta elettronica certificata.

2. Le richieste di notifica effettuate dai soggetti abilitati esterni sono inoltrate all'UNEP tramite posta elettronica certificata, nel rispetto dei requisiti tecnici di cui agli articoli 16, 17 e 18; all'interno della busta telematica è inserito il file RichiestaParte.xml, il cui XML-Schema è riportato nell'Allegato 5.

3. All'UNEP può essere inviata, sempre all'interno della busta telematica, la richiesta di pignoramento il cui XML-Schema è riportato nell'Allegato 5.

4. Alla notificazione per via telematica da parte dell'UNEP si applicano le specifiche della comunicazione per via telematica di cui all'articolo 20; il formato del messaggio di posta elettronica certificata è riportato nell'Allegato 7.

5. Ai fini della notificazione per via telematica, il sistema informatico dell'UNEP recupera l'indirizzo di posta elettronica del destinatario a seconda della sua tipologia:

a) soggetti abilitati esterni e professionisti iscritti in albi o elenchi costituiti ai sensi dell'articolo 16 del decreto-legge 29 novembre 2008, n. 185 convertito con legge del 28 gennaio 2009, n. 2: dal

ReGIndE, ai sensi dell'articolo 7, comma 6, nonché dall'indice nazionale delle imprese e dei professionisti (INI-PEC), sezione professionisti;

b) imprese iscritte nel relativo registro: ai sensi dell'articolo 7, comma 5;

c) cittadini: ai sensi dell'articolo 7, comma 5.

6. Il sistema informatico dell'UNEP, eseguita la notificazione, trasmette - per via telematica a chi ha richiesto il servizio - il documento informatico con la relazione di notificazione sottoscritta mediante firma digitale o firma elettronica qualificata e congiunta all'atto cui si riferisce, nonché le ricevute di posta elettronica certificata. La relazione di notificazione è in formato XML e rispetta l'XML-Schema riportato nell'Allegato 5; se il richiedente è un soggetto abilitato esterno, la trasmissione avviene via posta elettronica certificata; il formato del messaggio è riportato nell'Allegato 7.

7. La casella di posta elettronica certificata di un soggetto abilitato esterno deve disporre di uno spazio disco minimo pari a 1 Gigabyte.

Articolo 23

(Richiesta di copie di atti e documenti nel procedimento civile)

1. Per la richiesta telematica di copie di atti e documenti relativi al procedimento da parte dei soggetti non abilitati è disponibile, sul punto di accesso e sul PST, un servizio sincrono attraverso il quale individuare i documenti di cui richiedere copia e, in seguito al perfezionamento del pagamento, inoltrare la richiesta effettiva della copia stessa.

2. Il soggetto che ne ha diritto può richiedere alla cancelleria:

a) copia semplice in formato digitale;

b) copia semplice per l'avvocato non costituito in formato digitale;

c) copia autentica in formato digitale;

d) copia esecutiva in formato digitale;

e) copia semplice in formato cartaceo;

f) copia autentica in formato cartaceo;

g) copia esecutiva in formato cartaceo.

3. I dati relativi alla richiesta sono inoltrati all'ufficio giudiziario attraverso l'invocazione di un apposito web service; al richiedente è restituito l'identificativo univoco della richiesta inoltrata. Tale identificativo univoco è associato all'intero flusso di gestione della richiesta e di rilascio della copia.

4. Nel caso in cui la copia non possa essere rilasciata il sistema, in maniera automatica, comunica al richiedente l'impossibilità di evadere la richiesta.

Articolo 24

(Rilascio delle copie di atti e documenti)

1. Il rilascio della copia informatica di atti e documenti viene eseguito secondo le specifiche di cui all'articolo 16 del regolamento e dell'articolo 23-bis del CAD; la copia è inviata al richiedente in allegato ad un messaggio di posta elettronica certificata, secondo il formato riportato nell'Allegato 9.

2. Nel caso di copia di documenti contenenti dati sensibili o nel caso di copia di documenti che eccedono il massimo consentito dalla posta elettronica certificata, il messaggio di cui al comma precedente contiene l'avviso di disponibilità della copia, secondo il formato riportato nell'Allegato 9; il prelievo avviene secondo le specifiche di cui all'articolo 25, commi 2, 3 e 4.

CAPO IV

CONSULTAZIONE DELLE INFORMAZIONI DEL DOMINIO GIUSTIZIA

Articolo 25

(Requisiti di sicurezza)

1. L'architettura dei servizi di consultazione aderisce al modello MVC (Model View Controller) e prevede il disaccoppiamento del front-end, localizzato sul punto di accesso o sul PST, dal back-end, localizzato sul gestore dei servizi telematici, incaricato di esporre i servizi sottoforma di web service (http/SOAP).

2. Il PST espone, attraverso un apposito servizio proxy, i web service forniti dal gestore dei servizi telematici, a beneficio dei punti di accesso e di applicazioni esterne.

3. I punti di accesso realizzano autonomamente la parte di front-end, che deve essere localizzata all'interno della intranet del PdA stesso e non deve essere accessibile direttamente dall'esterno.

4. I punti di accesso possono a loro volta esporre i web service forniti dal gestore dei servizi telematici, a beneficio di applicazioni esterne.

5. Il protocollo di trasporto tra il punto di accesso e il proxy è HTTPS; la serializzazione dei messaggi è nel formato XML/SOAP.

6. Le funzionalità fornite dai web service realizzati, nonché le relative regole di invocazione, sono descritte tramite i WSDL pubblicati sull'area pubblica del PST.

7. L'accesso ai servizi di consultazione avviene su canale sicuro (protocollo SSL) previa identificazione informatica su di un PdA o sul PST, secondo le specifiche di cui all'articolo 6; a seguito di tale identificazione, il PdA o il PST attribuiscono all'utente un ruolo di consultazione, a seconda del registro di cancelleria; eseguita tale operazione, viene trasmesso al proxy di cui al comma 2 il codice fiscale del soggetto che effettua l'accesso (nell'header http) e il ruolo di consultazione stesso (nel messaggio SOAP); il proxy trasmette la richiesta al web service del gestore dei servizi telematici.

8. In base al ruolo di consultazione di cui al comma precedente, il sistema fornisce le autorizzazioni all'accesso rispetto alle informazioni anagrafiche contenute nei sistemi di gestione dei registri o sulla base dell'atto di delega previsto dal regolamento.

9. In fase di richiesta di attivazione, il punto di accesso può adottare meccanismi di identificazione basati sulla gestione federata delle identità digitali (modello GFID), secondo le specifiche dell'Agenzia per l'Italia Digitale; in questo caso, il Direttore generale DGSIA, valutata la soluzione proposta e opportunamente descritta nel piano della sicurezza, approva il meccanismo di identificazione che soddisfa il livello di sicurezza richiesto.

10. Il punto di accesso può consentire l'accesso a soggetti delegati da un utente registrato (soggetto delegante), con le stesse modalità di cui ai commi 7, 8 e 9, purché il soggetto delegante abbia predisposto un atto di delega, sottoscritto con firma digitale, che il punto di accesso conserva

per cinque anni unitamente alla tracciatura di ogni accesso effettuato su delega; le informazioni e gli atti di cui sopra sono forniti su richiesta al Ministero della giustizia.

11. Fuori dai casi previsti ai commi 1 e 10, l'architettura dei servizi di consultazione prevede in via residuale che il PdA o il PST effettuino, a seguito dell'identificazione di cui al comma 7, un link diretto dalle proprie pagine alla pagina principale del sito web che rende disponibili i servizi su canale sicuro (HTTPS); in questo caso i dati identificativi del soggetto vengono inseriti nell'header HTTP della richiesta.

12. I servizi di consultazione attivi sono elencati, per singolo ufficio, nel catalogo dei servizi telematici, di cui all'articolo 5, comma 5.

13. L'elenco dei PdA autorizzati è pubblicato nell'area pubblica del PST e nel catalogo dei servizi telematici, di cui all'articolo 5, comma 5.

14. Il PdA si dota di un piano della sicurezza, depositato al responsabile per i sistemi informativi automatizzati unitamente all'istanza di iscrizione all'elenco pubblico dei punti di accesso, che prevede la trattazione, esaustiva e dettagliata, dei seguenti argomenti:

a) struttura logistica e operativa dell'organizzazione;

b) ripartizione e definizione delle responsabilità del personale addetto;

c) descrizione dei dispositivi installati;

d) descrizione dell'infrastruttura di protezione, per ciascun immobile interessato (e rilevante ai fini della sicurezza);

e) descrizione delle procedure di registrazione delle utenze;

f) descrizione relativa all'implementazione dei meccanismi di identificazione informatica;

g) qualora il PdA integri la gestione delle caselle di PEC dei propri utenti, descrizione delle modalità di integrazione;

h) procedura di gestione delle copie di sicurezza dei dati;

i) procedura di gestione dei disastri;

j) analisi dei rischi e contromisure previste;

k) descrizione dell'eventuale processo di delega di cui al comma 10 nonché delle modalità di conservazione dell'elenco dei soggetti delegati e delle eventuali revoche delle deleghe;

l) descrizione della modalità di verifica dell'effettiva funzionalità e adeguatezza del sistema di sicurezza del punto di accesso.

15. Ai fini dell'iscrizione nel suddetto elenco, il responsabile per i sistemi informativi automatizzati verifica il piano della sicurezza di cui al comma precedente e può disporre apposite verifiche in loco, in particolare per accertare il rispetto delle prescrizioni di sicurezza riportate nel presente provvedimento.

16. Il punto di accesso abilita i propri iscritti unicamente a usufruire dei servizi esplicitamente autorizzati dal responsabile per i sistemi informativi automatizzati e riportati nel catalogo dei servizi telematici.

17. Il PdA si dota di una casella di posta elettronica certificata, che comunica al responsabile per i sistemi informativi automatizzati, da utilizzarsi per inviare e ricevere comunicazioni con il Ministero della giustizia.

18. Il PdA fornisce al Ministero della giustizia, su richiesta, i dati di censimento sul ReGIndE di cui articolo 8 comma 1 per i casi di iscrizione dei professionisti non iscritti in albi di cui articolo 9 comma 1.

19. Il PdA verifica l'effettiva funzionalità e adeguatezza del sistema di sicurezza almeno una volta l'anno e provvede ad inviare l'esito delle stesse, unitamente ad eventuali variazioni nei contenuti del piano, all'indirizzo di posta elettronica certificata del responsabile per i sistemi informativi automatizzati: prot.dgsia.ddsc@giustiziacert.it.

Articolo 26

(Registrazione dei soggetti abilitati esterni e degli utenti privati)

1. L'utente accede ai servizi di consultazione previa registrazione presso un PdA autorizzato o presso il PST.

2. Il PdA o il PST effettuano la registrazione del soggetto abilitato esterno o dell'utente privato, prelevando il codice fiscale dal token crittografico dell'utente; attraverso un'apposita maschera web, l'utente (senza poter modificare il codice fiscale) completa i propri dati, inserendo almeno le seguenti informazioni:

a) nome e cognome

b) luogo e data di nascita

c) residenza

d) domicilio

e) ruolo

f) consiglio dell'ordine o ente di appartenenza.

3. I dati di cui al comma precedente, unitamente alla data in cui è avvenuta la registrazione, sono archiviati e conservati per cinque anni.

4. Gli esperti e gli ausiliari del giudice, non iscritti ad alcun albo professionale o per i quali il proprio ordine non abbia provveduto all'invio dell'albo, presentano, all'atto della registrazione, copia elettronica in formato PDF dell'incarico di nomina da parte del giudice; tale copia è sottoscritta con firma digitale o firma elettronica qualificata dal soggetto che s'iscrive.

5. Qualora il professionista sia iscritto ad un albo dei consulenti tecnici, istituito presso un tribunale, al PdA viene presentata copia elettronica in formato PDF del provvedimento di iscrizione all'albo stesso da parte del comitato; tale copia è sottoscritta con firma digitale o firma elettronica qualificata dal soggetto che si iscrive.

6. Il PdA è tenuto a conservare i documenti informatici di cui ai commi precedenti, e a renderli disponibili, su richiesta, al Ministero della giustizia.

7. I PdA trasmettono al Ministero della giustizia le informazioni relative ai propri utenti registrati secondo le modalità di cui all'allegato 11.

CAPO V

PAGAMENTI TELEMATICI

Articolo 27

(Requisiti relativi al processo di pagamento telematico)

1. Il PST espone ai punti di accesso servizi web per l'esecuzione dei pagamenti telematici utilizzando le funzionalità messe a disposizione dal Nodo dei Pagamenti-SPC.

2. Le funzionalità fornite dai web service realizzati, nonché le relative regole di invocazione, sono descritte tramite i WSDL pubblicati sull’area pubblica del PST.